UNITED STATES DISTRICT COURT

DISTRICT OF MINNESOTA

SCOTT G. SAVEDOW, Individually and on Behalf of All Others Similarly Situated,

Plaintiff,

vs.

TARGET CORPORATION,

Defendant.

_____/

CIVIL NO. _____

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Scott Savedow ("Plaintiff"), individually and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to him and on information and belief as to all other matters, and upon the investigation conducted by Plaintiff's counsel, Robbins Geller Rudman & Dowd LLP, as detailed below, brings this class action complaint against Target Corporation (the "Company" or "Defendant" or "Target"), and alleges as follows:

INTRODUCTION

1. This nationwide class action arises from the ***second largest*** data security breach in U.S. history. In November and December, 2013, Target sustained one or more massive security breaches to its computer systems, servers, and databases (the "Network").

2. These security breaches (collectively, the "Data Breach" or "Breach") placed sensitive personal and financial information in the hands of cyber criminals, including, but not limited to, customer names, mailing addresses, as well as credit and debit card numbers, expiration dates, CVV codes, security codes, other personal information (collectively, "Personal Information").

3. Target was entrusted with the Personal Information of Plaintiff and other Class members (defined below). Target has a duty to maintain reasonable and adequate security measures to secure, protect, and safeguard their Personal Information stored on its Network. Target breached that duty by exposing Plaintiff's and the other Class members' Personal Information on an inadequately protected Network.

4. As the result of Target's failure to secure its Network, the Data Breach occurred and Plaintiff's and the other Class members' Personal Information was compromised, causing them to suffer from fraud and identity theft, and causing direct financial expenses associated with credit monitoring, replacement of compromised credit, debit or bank card numbers, and other measures needed to remedy fraud and identify theft that already occurred and to protect against further fraud arising from the Data Breach.

5. Plaintiff and the other Class members have also been deprived of the full use of certain of their debit cards, as large financial institutions, including JP Morgan Chase and Santander Bank, have instituted spending limits or other restrictions on debit cards that were used at Target during the Data Breach.

PARTIES

6. Plaintiff Scott G. Savedow resides in Broward County, Florida and is a citizen of the state of Florida. Plaintiff used his Visa Debit Card issued by Brightstar Credit Union on multiple occasions at a Target stores located in Sunrise, Florida and Lauderhill, Florida between November 29, 2013 and December 9, 2013. Plaintiff first learned that his Personal Information had been compromised by the Data Breach when he received a call in mid-December 2013 that his debit card had been used in Colorado. As a result of the Data Breach, Plaintiff's Personal Information was stolen, he directly suffered from identity theft and fraud, and is exposed to future and likely ongoing fraud as well.

7. Target is a Minnesota Corporation with its principle place of business at 1000 Nicollet Mall, Minneapolis, Minnesota 55403.

JURISDICTION AND VENUE

8. The Court has subject matter jurisdiction over this class action pursuant 28 U.S.C. §1332(d), because Plaintiff and the other Class members are of diverse citizenship from one or more Defendants; there are more than 100 Class members nationwide; and the aggregate amount in controversy exceeds five million dollars ($5,000,000.00), excluding interest and costs.

9. Venue is proper in this District under 28 U.S.C. §1391 because Defendant engaged in substantial conduct relevant to Plaintiff's claims within this District and have caused harm to Class members residing within this District.

SUBSTANTIVE FACTUAL ALLEGATIONS

A. Target Corporation

10. Target, the second largest general merchandise retailer in America, is self-described as an upscale discount retailer that provides high-quality, on-trend merchandise at attractive prices in clean, spacious and guest-friendly stores. Target has 1,797 stores in the United States, 124 stores in Canada and 37 distribution centers. Target boasts over 360,000 team members worldwide.[1]

[1] *See* http://pressroom.target.com/corporate (*last visited on* December 23, 2013).

11. Target also maintains a website, TARGET.COM, where customers can search for and purchase thousands of products. TARGET.COM is consistently ranked as one of the most-visited retail websites.[2]

12. Target's revenues have steadily increased from $64.9 billion in 2008 to $73.3 billion in 2012.[3]

13. According to Target's Privacy Policy, Target "maintain[s] administrative, technical and physical safeguards to protect your personal information. When we collect or transmit sensitive information such as a credit or debit card number, we use industry standard methods to protect that information."[4]

14. Target's promise of protection of admittedly sensitive personal information, however, was all a lie.

B. The Breach

15. On December 18, 2013, online sources first reported that Target was ***conducting an investigation*** into a possible data breach.[5]

16. According to a report written by Brian Krebs, Target was "investigating a data breach potentially involving millions of customer credit and debit card records," which occurred on or near November 29, 2013 ("Black Friday").[6]

---

[2] *See id*.

[3] *See* Target Corp. 2012 Form 10-K, p. 14.

[4] *See* http://www.target.com/spot/privacy-policy (*last visited on* December 23, 2013).

[5] Brian Krebs, of KREBSONSECURITY.COM, appears to be the first to report the Data Breach.

17. The following day, on December 19, 2013, Target issued a press release which confirmed that unauthorized persons gained access to payment card data from U.S. stores. The release stated that "[a]pproximately 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013."[7]

18. Coverage of the Data Breach became widespread on December 19, 2013, following the announcement by Target.[8]

19. In a separate December 19, 2013 statement, Target admitted that, at a minimum, the Data Breach "included customer name, credit or debit card number, and the card's expiration date and CVV [Card Verification Value]."[9] However, the full extent of the Data Breach has likely yet to be revealed as Target continues its internal investigation.

20. On December 20, 2013, Target began notifying customers affected by the Data Breach, although the reach of this notice is unclear at the present time.

---

[6] *See* http://money.cnn.com/2013/12/18/news/companies/target-credit-card/ (*last visited on* December 23, 2013); http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/ (*last visited on* December 26, 2013).

[7] *See* http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores (*last visited on* December 25, 2013).

[8] *See*, *e.g.*, The New York Times, http://www.nytimes.com/2013/12/20/technology/target-stolen-shopper-data.html?adxnnl=1&adxnnlx=1387897818-hSv1vHJK5gXtqLYADjMXVg (*last visited on* December 25, 2013); The Wall Street Journal, http://online.wsj.com/news/articles/SB10001424052702304367204579267992268980478 (*last visited on* December 25, 2013); FOX News, http://www.foxnews.com/us/2013/12/19/target-says-40m-accounts-may-be-affected-by-data-breach/ (*last visited on* December 25, 2013).

[9] *See* https://corporate.target.com/discover/article/Important-Notice-Unauthorized-access-to-payment-ca (*last visited on* December 25, 2013).

21. Although the exact method of the breach has not been disclosed by Target, reports suggest that hackers targeted the Company's point-of-sale system. Meaning, the hackers either slipped malware into the terminals where customers swipe their credit and debit cards or collected customer data while it was on route from Target to its credit and debit card processors.[10]

22. The effects of the Data Breach are already apparent. For instance, Brain Krebs of KREBSONSECURITY.COM reported, on December 20, 2013, about the illegal black market sale of Credit Card numbers obtained as a result of the Data Breach. According to Krebs, the Credit Card numbers were already on sale online, "ranging in price from $26.60 to $44.80 apiece." Further, buyers were provided with the ZIP code and city of the store from which the cards were stolen.[11]

23. Additionally, as warnings are being issued by Target and other media outlets to check for suspicious charges on credit, debit or bank cards affected by the Data Breach, Target customers are beginning to see such fraudulent charges on their cards.[12]

---

[10] *See* http://money.cnn.com/2013/12/18/news/companies/target-credit-card/index.html (*last visited on* December 25, 2013).

[11] *See* http://investing.businessweek.com/research/stocks/news/article.asp?docKey=600-201312201721KRTRIB__BUSNEWS_31255_35377-1&ex=true&ticker=JWN (*last visited on* December 25, 2013); http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/ (*last visited on* December 25, 2013).

[12] *See* https://corporate.target.com/discover/article/Important-Notice-Unauthorized-access-to-payment-ca (*last visited on* December 25, 2013); http://news.msn.com/us/how-to-handle-targets-data-breach (*last visited on* December 25, 2013).

24. As of December 23, 2013, the Department of Justice began an investigation into the Data Breach, according to Target. Target has stated that it is cooperating in the investigation.[13]

25. The next day, Reuters reported that, contrary to Target's public representations that no "PIN data, whether encrypted or unencrypted, was compromised," "[t]he hackers who attacked Target . . . and compromised up to 40 million credit cards and debit cards [did manage] to steal encrypted personal identification numbers (PINs), according to a senior payments executive familiar with the situation."[14]

26. The Reuters article continued:

> While bank customers are typically not liable for losses because of fraudulent activity on their credit and debit cards, JPMorgan Chase & Co (JPM.N) and Santander Bank (SAN.MC) said they have lowered limits on how much cash customers can take out of teller machines and spend at stores.
>
> The unprecedented move has led to complaints from consumer advocates about the inconvenience it caused from the late November Thanksgiving holiday into the run-up to Christmas. But sorting out account activity after a fraudulent withdrawal could take a lot more time and be worse for customers.

C. Impact of the Breach on Plaintiff

27. Plaintiff has regularly shopped at Target over the past several years, and trusted that, as Target promised, the Company would provide adequate safeguards to protect Plaintiff's sensitive personal information from being stolen or misused.

---

[13] *See* http://www.foxnews.com/us/2013/12/23/target-says-justice-department-investigating-credit-and-debit-card-security/ (*last visited on* December 24, 2013).

[14] *See* http://www.reuters.com/article/2013/12/24/us-target-databreach-idUSBRE9BN0L220131224 (*last visited* December 26, 2013).

28. Plaintiff shopped at a Target location in Sunrise, Florida location (Store #T0815) on November 29, 2013, and shopped at a Target location in Lauderhill, FL (Store #T1778) on December 9, 2013.

29. On December 14, 2013, Plaintiff received a phone call from the credit union that issued his Visa debit card (the "Card Issuer") inquiring about several recent charges or transactions emanating from Colorado that were posted to his account. Plaintiff confirmed that the stated transactions were not performed by him and were unauthorized. The unauthorized transactions were as follows:

Date	Type of Withdrawal	Location	Amount
12/13/2013	Network ATM Fee	Edwards Village, CO	$2.00
12/13/2013	ATM Withdrawal	Edwards Village, CO	$503.00
12/13/2013	Network ATM Fee	Edwards Village, CO	$2.00
12/14/2013	ATM Withdrawal	Vail, CO	$243.00
12/14/2013	Network ATM Fee	Vail, CO	$2.00

30. As of the described December 14, 2013 phone call, Plaintiff did not receive any communication from Target about the Data Breach. As of that date, Target, likewise, did not issue any notice or public announcement about the Data Breach.

31. On December 15, 2013, Plaintiff had a follow-up call with a representative of the Card Issuer. He was asked to again verify the Colorado charges or transactions. Plaintiff again confirmed that the stated transactions were not performed by him and were unauthorized.

32. As of the described December 15, 2013 phone call, Plaintiff did not receive any communication from Target about the Data Breach. As of that date, Target, likewise, did not issue any notice or public announcement about the Breach.

33. Immediately after learning of the unauthorized transactions on his Visa debit card, Plaintiff checked his balance. He substantiated that his account had, in fact, been hacked and that more than $750 dollars had been withdrawn by an unauthorized user.

34. Plaintiff was first notified by Target of the Breach on or about December 20, 2013.

35. As of the filing of this Complaint, as a result of the Breach, Plaintiff remained in the process of disputing the improper transactions to his account, and has not been reimbursed for his losses.

36. In addition, Plaintiff remains at risk for overdraft charges in the event automatic bills paid from his debit card account are paid with insufficient funds.

D. The Data Breach and Target's Failure to Disclose

37. On information and belief, sometime during November and December, 2013, a hacker, or a group of hackers carried out a cyber-attack on Target's Network. During this attack, the hackers accessed and stole the Personal Information of millions of Target customers, including Plaintiff and the other Class members.

38. Target knew or should have known that its servers, systems, and Network were not secure and left Plaintiff's and the other Class members' Personal Information vulnerable to attack, theft, and misuse.

39. Online sources first reported that Target was ***conducting an investigation*** into a possible data breach on December 18, 2013.

40. It is not clear, based on publicly available information or through statements made by Target, when Target first became aware of the breach.

41. Upon information and belief, however, Target was aware of the Breach in advance of its December 19, 2013 press release announcing the Data Breach.

42. It is not clear, based on publicly available information or through statements made by Target, whether Target only released this information in response to reports – online or otherwise – regarding the Data Breach.

E. Target Knew of Should Have Known That Its Network was Vulnerable to Attack

43. Target knew or should have known that its less than industry-standard security systems and unreasonably vulnerable technologies would render its Network an aim of attacks by third-parties. Target, however, failed to take corrective measures to update its systems and technologies.

44. Despite the ever-existing threat of a security breach, Target unreasonably and unfairly failed to implement adequate safeguards to protect its Network, including failing to take steps to protect Plaintiff's and the other Class members' Personal Information stored on its Network.

F. Target Failed to Implement Basic Security Measures that Would Have Prevented the Data Breach

45. On information and belief, Target had not implemented reasonable, industry-standard, or appropriate security measures and knowingly, recklessly, or as a matter of gross negligence left Plaintiff's and the other Class members' Personal

Information stored on its Network vulnerable to one of the largest cyber-attacks and data thefts in history.

46. Despite Target's duty to take reasonable steps to secure its Network, it in fact failed to take reasonable and adequate measures to protect Plaintiff's and the other Class members' Personal Information stored on its Network.

47. On information and belief, among Target's failures in this respect were its failure to maintain adequate backups and/or redundant systems; failure to encrypt data and establish adequate firewalls to handle a server intrusion contingency; and failure to provide prompt and adequate warnings of security breaches.

G. Significance of Protecting Personal Information of Plaintiff and Members of the Class

48. Consumers have a vested interest in protecting all of their confidential or private information, ranging from bank account information, credit card information, debit card information, social security numbers, asset information and the like.

49. The significant impact identity theft can have on consumers and the extreme financial ramification the failure to secure personal information can cause has led to the enactment of numerous privacy-related laws aimed toward protecting consumer information and disclosure requirements, including, for example: (1) Gramm-Leach-Bliley Act; (2) Fair Credit Reporting Act; (3) Fair and Accurate Credit Transactions Act; (4) Federal Trade Commission Act, 15 U.S.C. §§41-58; (5) Driver's Privacy Protection Act; (6) Health Insurance Portability and Accountability Act; (7) The Privacy Act of

1974; (8) Social Security Act Amendments of 1990; (9) E-Government Act of 2002; and (10) Federal Information Security Management Act of 2002.

50. Protection of consumers' private information is obviously critical. Consumers are at the mercy of the security measures or controls utilized by those entities that use or maintain their confidential or private information. Consumers, likewise, have no ability to ascertain whether their private information is being adequately protected or, worse, if their private information has been compromised, in any way. Where, as here, Personal Information is and has been inadequately protected and the entity maintaining that information conceals the inadequate safety measures and possibility that a breach occurred or is occurring, consumers become highly vulnerable to identity theft.

H. The Data Breach, Caused by Target's Improper Conduct, Has Harmed Plaintiff and the Other Class Members

51. As a result of the Data Breach, Plaintiff and Class members now face years of hardship, through existing identity theft and fraud, as well as constant fear and threat of additional identity theft or other internet-based harassment, not to mention the restriction or complete loss of use of their credit or debit cards, constant surveillance of financial and personal records, as well as constant monitoring of their credit reports.

1. Identity Theft

52. As a result of the Data Breach, cyber-criminals now possess the Personal Information of Plaintiff and the other Class members. While credit card companies offer protection against unauthorized charges, the process is long, costly, and frustrating. Physical cards must be replaced, credit and debit card information must be updated on all

automatic payment accounts, and victims must add themselves to credit fraud watch lists, which substantially impairs victims' ability to obtain additional credit. Immediate notice of the breach is essential to obtain the best protection afforded by these services. In this instance, the Data Breach included, but was not limited to, customer names, mailing addresses, as well as credit and debit card numbers, expiration dates, security codes, pin numbers and other personal information. Having information, such as pin numbers, could enable hackers to gain access to other accounts of the Plaintiff and Class members.

53. Further, as alleged above, Target failed to provide such immediate notice, thus further exacerbating the damages sustained by Plaintiff and the other Class members arising from the Data Breach.

54. Companies recognize that Personal Information is a valuable asset. Indeed, Symantec Corporation has even created a software application that values a person's identity on the black market.[15]

55. Personal Information is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen credit card numbers, Social Security numbers, and other personally identifiable information on a number of Internet websites. As one industry report recognized, this "credit card black-market operates very much in the open" and a number of websites exist that offer stolen credit card numbers and associated credentials. The report went on to state:

[15] *See* Risk Assessment Tool, Norton 2010, http://www.everyclickmatters.com/victim/assessment-tool.html; *see also* T. Soma, *et al.*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009); http://law.richmond.edu/jolt/v15i4/article11.pdf.

> It is clear from the current state of the credit card black-market that cyber criminals can operate much too easily on the Internet. They are not afraid to put out their email addresses, in some cases phone numbers and other credentials in their advertisements. It seems that the black market for cyber criminals is not underground at all. In fact, it's very "in your face."[16]

56. As alleged above, Plaintiff's account has already been improperly accessed and used. As a result, Plaintiff's vulnerability to identity theft is not speculative. It is tangible.

2 Loss or Restriction of Use of Certain Debit Cards

57. In the wake of a security breach regarding Personal Information, financial institutions often try to stay in front of criminals who attempt to use fraudulently obtained credit, debit or bank card information.

58. Indeed, certain financial institutions, whose users were subject to the Data Breach, are implementing such measures. As such, customers are being affected in that they are unable to use their debit cards as intended. For instance, as a result of the Data Breach, JP Morgan Chase notified customers who used Chase brand debit cards at Target from November 27 through December 15, that they were limited to $100 a day of cash withdrawals and $300 a day of purchases with their cards. International travelers were completely restricted from accessing cash from foreign ATMs. These limits affects roughly 2 million accounts, or 10 percent of Chase Debit Cards.[17] These limits are dramatically lower than the standard $500 a day of cash withdrawals and $500 a day of

---

[16] *See* http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/ (*last visited on* December 25, 2013).

[17] *See* http://www.chicagotribune.com/business/breaking/chi-chase-limits-target-debit-20131221,0,4134532.story (*last visited on* December 25, 2013).

purchases.[18] Consequently, the Data Breach has resulted in a reduction of credit by the Class.

59. Additionally, other institutions, including Bank of America Corp. and Citigroup Inc. indicated that their institutions were taking steps to protect accounts, but none described specific actions to limit the use of affected cardholder's credit, debit, or bank cards.[19]

60. This restrictions or limitations directly affect the customers who debit cards were subject to the Data Breach, by creating nuisances to their daily lives. First, debit card users are unable to access their own cash, which is contained within their own bank account, via their debit card. As such, these debit card users are restricted access to cash they may need to pay for living or other expenses. Second, debit card users abroad are totally prevented from using their debit cards to withdraw money from foreign ATMs.

61. These measures are especially burdensome around the holiday season, when people need access to cash to pay for things commonly purchased, like presents and gifts. Indeed, Chase, in the notice it provided to its affected customers, stated that the restrictions "could not have happened at a more inconvenient time with the holiday season upon us."[20]

---

[18] *See* http://www.reuters.com/article/2013/12/21/us-target-jpmorgan-idUSBRE9BK0D02013 1221 (*last visited on* December 25, 2013).

[19] *See* http://www.chicagotribune.com/business/breaking/chi-chase-limits-target-debit-20 131221,0,4134532.story (*last visited on* December 25, 2013).

[20] *See* http://www.reuters.com/article/2013/12/21/us-target-jpmorgan-idUSBRE9BK0D02013 1221 (*last visited on* December 25, 2013).

3. Continued Credit Monitoring

62. Credit monitoring is a service that tracks a person's credit report on a daily basis and notifies that person of any significant changes on their report. These credit monitoring services will notify a consumer any time a new account is opened in their name, can help prevent error from credit reports, and most notably, credit monitoring will notify a consumer of derogatory reports such as a delinquencies from a creditor.

63. As a result of the Data Breach, Plaintiff and Class members will be forced to engage in the monitoring of their credit, to ensure that customers: (1) detect any fraudulent charges; (2) detect any instances of new accounts being opened; and (3) report such instances to their credit card companies upon detection.

64. Credit monitoring services, such as IdentityGuard.Com or PrivacyGuard cost upwards of $14.99 per month for their credit monitoring services.

65. Based on the fact that Plaintiff's account has already been compromised, as alleged herein, he will be forced to engage in the monitoring of his credit.

4. Credit Score Affected

66. A credit score is a three-digit number generated by a mathematical algorithm using information in a person's credit report. It is designed to predict risk – specifically, the likelihood that a consumer will become seriously delinquent on your credit obligations in the 24 months after scoring.

67. A person's credit score is based on the following: (a) payment history (a person's account payment information, including any delinquencies); (b) amounts owed (how much is owed on a person's accounts); (c) length of credit history (when a person

opened their accounts and the time since a person's last account activity); (d) new credit (a person's pursuit of new credit, including credit inquiries and the number of recently opened accounts; and (e) types of credit used (the mix of a person's accounts, including revolving and installment).

68. A person's credit score directly impacts the ease and ability of that person to obtain credit. The higher a person's credit score, the easier the person will be able to obtain credit and the cheaper they will be able to obtain it for (in the form of interest rates).

69. Identity theft can have a direct impact on a person's credit score. For instance, a high balance, or high credit utilization, can drop a FICO credit score by as much as 45 points. Further, the opening of new, fraudulent, accounts under a person's name can cause a drop in a person's credit score. Relatedly, often times when these fraudulent accounts are opened, the affected person is unaware of the account, and as a result, fails to pay the resulting bills on time. Late payments can lead to a drop of a much as 100 points in a person's credit score.

70. While it may be possible to correct these errors which occur to a person's credit score, the short term affects are real, and can affect your credit score for months until the fraudulent actions are rectified, directly impact a person's ability to obtain credit to make necessary purchases in his or her life.

CLASS ACTION ALLEGATIONS

71. Plaintiff brings this lawsuit on behalf of himself and as a class action, pursuant to Rules 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure, on behalf of a proposed class (the "Class"), defined as:

> All persons or entities in the United States that used a Credit, Debit, or other Bank Card at Target and suffered a disruption of service and/or breach of security to their personal information beginning on or about November 27, 2013.
>
> All persons or entities in Florida that used a Credit, Debit, or other Bank Card at Target and suffered a disruption of service and/or breach of security to their personal information beginning on or about November 27, 2013.

72. Excluded from the Class is Defendant, including any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant.

73. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

74. The members of the Class are so numerous that joinder of all members would be impracticable. Upon information and belief, there are approximately 40 million customers impacted by the Data Breach. While the exact number of Class members is currently unknown to Plaintiff, upon information and belief, Plaintiff alleges that there are, at least, millions of Class members who were damaged by Target's conduct

described herein. The names and addresses of Class members are identifiable through documents maintained by Target. Ultimately, the sheer number of Class members, who are geographically dispersed around the United States, makes joinder of all members impracticable.

75. Common questions of law and fact exist as to all Class members and predominate over any questions which affect only individual Class members. These Common questions of law and fact include:

(a) whether Target engaged in the wrongful conduct alleged herein;

(b) whether Target owed a legal duty to Plaintiff and the other Class members to exercise due care in collecting, storing, and safeguarding their Personal Information;

(c) whether Target negligently or recklessly breached legal duties owed to Plaintiff and the other Class members to exercise due care in collecting, storing, and safeguarding their Personal Information;

(d) whether Target failed to implement and maintain reasonable securities practices and procedures to protect against the Data Breach;

(e) whether Target's conduct was negligent or willful;

(f) whether Target was unreasonable in its delay of notifying affected customers of the Data Breach;

(g) whether Target violated the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq.*;

(h) whether Target violated Minn. Stat. §325D.44;

(i) whether Plaintiff and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

(j) whether Plaintiff and the other Class members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

76. Plaintiff's claims are typical of the claims of the other Class members because, among other things, Plaintiff and the other Class members were injured through the substantially uniform misconduct described above. Plaintiff herein is advancing the same claims and legal theories on behalf of himself and all other Class members, and there are no defenses available to Target that are unique to Plaintiff.

77. Plaintiff will fairly and adequately protect the interests of those Class members he seeks to represent and has no interests that are antagonistic to the interests of any other Class member. Plaintiff has retained counsel who have substantial experience and success in complex litigation, including the litigation of class actions and consumer protection claims, including privacy protection claims in the class action context.

78. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Target, making it impracticable for Class members to individually seek redress for Target's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized

litigation would create a potential for inconsistent or contradictory judgments, and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I

Negligence

79. Plaintiff repeats, realleges, and incorporates by reference the allegations contained above, as though fully stated herein.

80. Target owed a duty to Plaintiff and the other Class members to exercise reasonable care in safeguarding and protecting their Personal Information in its possession from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Target's security systems to ensure that Plaintiff's and the other Class members' Personal Information in Target's possession was adequately secured and protected. Target further had a duty to implement processes that would detect a breach of its security system in a timely manner.

81. Target had a duty to timely disclose to Plaintiff and the other Class members that their Personal Information had been or was reasonably believed to have been compromised. Timely disclosure was appropriate so that, among other things, Plaintiff and the other Class members could take appropriate measures to avoid unauthorized charges to their credit/debit card accounts, cancel or change usernames and

passwords on compromised accounts, and monitor their account information and credit reports for fraudulent activity.

82. Target breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' Personal Information in its possession by failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and the other Class members' Personal Information; failing to adequately monitor the security of the Network; allowing unauthorized access to Plaintiff's and the other Class members' Personal Information stored on the Network; and failing to recognize in a timely manner that the Network had been breached.

83. Target breached its duty to timely disclose that Plaintiff's and the other Class members' Personal Information in its possession had been, or was reasonably believed to have been, stolen or compromised.

84. But for Target's wrongful and negligent breach of its duties owed to Plaintiff and the other Class members, their Personal Information would not have been compromised, and use of credit, debit or bank cards would not have been restricted or limited.

85. The injury and harm suffered by Plaintiff and the other Class members was the reasonably foreseeable result of Target's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' Personal Information within its possession. Target knew or should have known that its systems and technologies for processing and securing Plaintiff's and the other Class members' Personal Information had security vulnerabilities.

86. As a result of Target's negligence, Plaintiff and the other Class members incurred economic damages relating to expenses for credit monitoring and loss of use of their credit, debit, or bank cards.

COUNT II

Negligence Per Se

87. Plaintiff repeats, realleges, and incorporates by reference the allegations contained above, as though fully stated herein.

88. Pursuant to the Gramm-Leach-Bliley Act, 15 U.S.C. §6801, Defendant had a duty to keep and protect the Personal Information of its customers.

89. Defendant violated the Gramm-Leach-Bliley Act by failing to keep and protect the Plaintiff's and Class members' Personal information, failing to monitor, and/or failing to ensure that Defendant complied with PCI data security standards, card association standards, statutes and/or other regulations to protect such Personal Information.

90. Defendant also failed to comply with PCI data security standards, card association standards, statutes and/or other regulations prohibiting the storage of unprotected Personal Information.

91. Defendant's failure to comply with the Gramm-Leach-Bliley Act, and/or other industry standards and regulations, constitutes negligence per se.

COUNT III

Breach of Implied Contract

92. Plaintiff repeats, realleges, and incorporates by reference the allegations contained above, as though fully stated herein.

93. The Personal Information of Plaintiff and the Class members was provided to Defendant to pay for goods purchased from Target or TARGET.COM. Implicit in this transaction was a covenant for Defendant to undertake reasonable efforts to safeguard, protect and secure this information. Also implicit in this transaction was a covenant for Defendant to promptly notify its customers in the event that this information was compromised or at risk.

94. Defendant's recognition of these covenants and obligations is implicit in their representations to Plaintiff and the Class regarding the importance of maintaining strong security measures to protect confidential information.

95. This implied contract required Defendant to safeguard the Personal Information of Plaintiff and the Class and prevent that information from being compromised and/or stolen.

96. Defendant did not safeguard and protect the private and confidential information of Plaintiff and the Class and failed to adequately prevent that information from being compromised or available for unauthorized dissemination. To the contrary, Defendant allowed (and continue to allow) this information to be disclosed to unauthorized parties.

97. As a result, Defendant breached its implied contract with Plaintiff and the Class, thereby causing injury to Plaintiff and the Class.

COUNT IV

Violation of Fla. Deceptive and Unfair Trade Practices Act, Fla. Stat. Section 501.201, *et seq.*, and the Unfair Trade Practices Statutes

98. Plaintiff repeats, realleges, and incorporates by reference the allegations contained above, as though fully stated herein.

99. At all relevant times, Defendant provided goods and/or services and thereby was engaged in trade or commerce.

100. At all relevant times, Plaintiff and the Class members were consumers.

101. Defendant was aware that its customers provided confidential and non-public information and personally identifiable material in connection with the purchase of goods from Target and Target.com.

102. Plaintiff and the Class expected, and Defendant assured, that Personal Information and non-public information maintained by Defendant would be protected and that it would not be disclosed to third parties.

103. Defendant engaged in unfair or deceptive acts and practices by knowingly permitting the Personal Information to be exposed through a Network that was unsecure or had inadequate safeguards, resulting in the dissemination of personal and private information of customers in direct violation of the Unfair Trade Practices Statutes.

104. Defendant engaged in unfair or deceptive acts and practices by failing to timely notify Plaintiff and the Class of the security breach and compromise.

105. Defendant's practice and course of conduct, as alleged herein, is likely to mislead – and has misled – the consumer acting reasonably in the circumstances, to the consumer's detriment.

106. Further, Defendant has engaged in an unfair practice that offends established public policy, and is one that is immoral, unethical, oppressive, unscrupulous and/or substantially injurious to customers.

107. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class members suffered actual damages and request a corresponding award of damages against Defendant, as authorized by such statutes.

108. In the alternative, Plaintiff and the Class members have suffered irreparable harm for which there is no adequate remedy at law as a result of Defendants' conduct and Plaintiff and the Class members are entitled to appropriate temporary and permanent injunctive relief, as authorized and provided by such statutes. Plaintiff and the Class members are further entitled to preliminary or other relief as provided by such statutes, including statutory damages, punitive damages, costs and reasonable attorneys' fees.

COUNT V

Violation of Minn. Stat. §325D.44 and the Unfair Trade Practices Statutes

109. Plaintiff repeats, realleges, and incorporates by reference the allegations contained above, as though fully stated herein.

110. Defendant was aware that its customers provided private information and personally identifiable material in connection with their purchases from Target and TARGET.COM.

111. Plaintiff and Class members expected, and Defendant assured, that confidential information maintained by Target would be protected and that it would not be disclosed to third parties.

112. Defendant engaged in unfair or deceptive acts and practices by knowingly permitting the confidential information to be exposed through the system they was unsecure or

had inadequate safeguards, resulting in the dissemination of personal and private information of customers in direct violation of Minn. Stat. §325D.44 and the Unfair Trade Practices Statutes.

113. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class members suffered actual damages and request a corresponding award of damages against Defendant, as authorized by Minn. Stat. §325D.44 and the Unfair Trade Practice Statutes.

114. In the alternative, Plaintiff and the Class members have suffered irreparable harm for which there is no adequate remedy at law as a result of Defendant's conduct and Plaintiff and the Class members are entitled to appropriate temporary and permanent injunctive relief, as authorized and provided by such statutes. Plaintiff and the Class members are further entitled to preliminary or other relief as provided by such statutes, including statutory damages, punitive damages, costs and reasonable attorneys' fees

COUNT VI

Bailment

115. Plaintiff repeats, realleges, and incorporates by reference the allegations contained above, as though fully stated herein.

116. Plaintiff and the other Class members delivered and entrusted their Personal Information to Target for the sole purpose of paying for items for sale in its stores or on TARGET.COM.

117. During the time of bailment, Target owed Plaintiff and the other Class members a duty to safeguard their Personal Information stored on its Network by maintaining reasonable security procedures and practices to protect such information. As alleged herein, Target breached this duty.

118. As a result of Target's breach of this duty, Plaintiff and the other Class members have been harmed as alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other Class members, respectfully request that this Court enter an Order:

A. Certifying the Class under Federal Rule of Civil Procedure 23(a), 23(b)(2), and 23(b)(3), appointing Plaintiff as Class Representative, and appointing his undersigned counsel as Class Counsel;

B. An award of equitable, injunctive and declaratory relief described herein, including judicial supervision of Defendant and a judicial determination of the rights and responsibilities of the parties regarding the remains that are the subject to this action;

C. Finding that Target's conduct was negligent, deceptive, unfair, and unlawful as alleged herein;

D. Enjoining Target from engaging in the negligent, deceptive, unfair, and unlawful business practices alleged herein;

E. Awarding Plaintiff and the other Class members actual, compensatory, and consequential damages;

F. Awarding Plaintiff and the other Class members statutory damages;

G. Awarding Plaintiff and the other Class members restitution and disgorgement;

H. Requiring Target to provide appropriate credit monitoring services to Plaintiff and the other Class members;

I. Awarding Plaintiff and the other Class members exemplary damages, should the finder of fact determine that Target acted with oppression, fraud, and/or malice;

J. Awarding Plaintiff and the other Class members pre-judgment and post-judgment interest;

K. Awarding Plaintiff and the other Class members reasonable attorneys' fees and costs, including expert witness fees; and

L. Granting such other relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

DATED: January 6, 2014

REINHARDT, WENDORF & BLANCHFIELD
GARRETT D. BLANCHFIELD, JR. (#209855)
BRANT D. PENNEY (#316878)

Garrett D. Blanchfield, Jr.
Garrett D. Blanchfield, Jr.

E-1250 First National Bank Bldg.
332 Minnesota St.
St. Paul, MN 55101
Telephone: 651/287-2100
651/287-2103 (fax)

ROBBINS GELLER RUDMAN
& DOWD LLP
STUART A. DAVIDSON
MARK J. DEARMAN
CHRISTOPHER C. MARTINS
120 East Palmetto Park Road, Suite 500
Boca Raton, FL 33432
Telephone: 561/750-3000
561/750-3364 (fax)
sdavidson@rgrdlaw.com
mdearman@rgrdlaw.com
cmartins@rgrdlaw.com

ROBBINS GELLER RUDMAN
& DOWD LLP
SAMUEL H. RUDMAN
ROBERT M. ROTHMAN
MARK S. REICH
WILLIAM J. GEDDISH
58 South Service Road, Suite 200
Melville, NY 11747
Telephone: 631/367-7100
631/367-1173 (fax)
rrothman@rgrdlaw.com
mreich@rgrdlaw.com
wgeddish@rgrdlaw.com

Attorneys for Plaintiff and the Class

G:\sdavidson\Target\Target CPT MN.docx